CIRCUITS AND METHODS FOR MODULAR EXPONENTIATION

ABSTRACT

The modular exponentiation function used in public key encryption and decryption systems is implemented in a standalone engine having at its core modular multiplication circuits which operate in two phases which share overlapping hardware structures. The partitioning of large arrays in the hardware structure, for multiplication and addition, into smaller structures results in a multiplier design comprising a series of nearly identical processing elements linked together in a chained fashion. As a result of the two-phase operation and the chaining together of partitioned processing elements, the overall structure is operable in a pipelined fashion to improve throughput and speed. The chained processing elements are constructed so as to provide a partitionable chain with separate parts for processing factors of the modulus. In this mode, the system is particularly useful for exploiting characteristics of the Chinese Remainder Theorem to perform rapid exponentiation operations. A checksum mechanism is also provided to insure accurate operation without impacting speed and without significantly increasing complexity. While the present disclosure is directed to a complex system which includes a number of features, the present application is particularly directed to circuits and methods for carrying out modular exponentiation.